

Summary of Changes
to
Procedure 200.3
Classified, Sensitive, and Proprietary Document Handling

Revised Version Issued as P 200.3B

LM Procedure 200.3A, Classified, Sensitive, and Proprietary Document Handling of 12/28/06, has undergone minor revision. The procedure has been revised to reflect updated definitions and provide additional guidance concerning the initial protection of material that may contain Classified Information. Please replace LM Procedure 200.3A with LM Procedure 200.3B.

U.S. Department of Energy Office of Legacy Management



Procedure: 200.3B

Effective: 11/1/07

SUBJECT: CLASSIFIED, SENSITIVE, AND PROPRIETARY DOCUMENT HANDLING

1. PURPOSE.

To provide personnel with instructions to properly identify and protect Classified, Sensitive, and Proprietary information.

2. CANCELLATION. Procedure 200.3A, Classified, Sensitive, and Proprietary Document Handling, dated 12/28/06

3. REFERENCES.

- a. 42 United States Code (U.S.C.) 2011-2259, Atomic Energy Act of 1954
- b. 10 Code of Federal Regulations (CFR) 710, Criteria and Procedures for Determining Eligibility for Access to Classified Matter or Special Nuclear Material
- c. 10 CFR 1017, Identification and Protection of Unclassified Controlled Nuclear Information
- d. 10 CFR 1045, Nuclear Classification and Declassification
- e. 32 CFR 2001, Classified National Security Information
- f. Executive Order 12958, Classified National Security Information
- g. U.S. Department of Energy (DOE) Manual 470.4-1, Safeguards and Security Program Planning and Management
- h. DOE Manual 470.4-2, Physical Protection

INITIATED BY: Office of Business Operations

NO. OF PAGES/ATTACHMENTS: 9 pages, 4 attachments

- i. DOE Manual 470.4-4, Information Security
- j. DOE Order 470.4, Safeguards and Security Program
- k. DOE Manual 471.1-1, Identification and Protection of Unclassified Controlled Nuclear Information Manual
- l. DOE Order 471.1, Identification and Protection of Unclassified Controlled Nuclear Information
- m. DOE Order 471.3, Identifying and Protecting Official Use Only Information
- n. DOE Manual 471.3-1, Manual for Identifying and Protecting Official Use Only Information
- o. DOE Manual 475.1-1, Identifying Classified Information

4. DEFINITIONS.

- a. Approved Security Container -- A security file container, originally procured from a Federal Supply Schedule supplier, which conforms to Federal specifications and bears a Test Certification Label on the locking drawer attesting to the security capabilities of the container and lock. Such containers will be labeled General Services Administration Approved Security Container on the outside of the top drawer.
- b. Classification Level -- A designation assigned to specific elements of information based on the potential damage to national security if disclosed to unauthorized persons. The three classification levels in descending order of potential damage are Top Secret, Secret, and Confidential.
- c. Classified Information -- Records or information requiring, for national security reasons, safeguards against unauthorized disclosure.
- d. Electronic Recordkeeping System (ERKS) -- An electronic information system in which records are collected, organized, and categorized to facilitate their preservation, retrieval, use, and disposition. An ERKS ensures that the records it maintains will have sufficient authenticity and reliability to meet the agency's recordkeeping requirements. These requirements are based in statute, ensuring "adequate and proper documentation," which contributes to efficient and economical agency operations.
- e. Incident of Security Concern -- Events that, at the time of occurrence, cannot be determined to be an actual violation of law, but which are of such significant concern to the DOE Safeguards and Security program as to warrant preliminary inquiry and subsequent reporting.

- f. LM Personnel -- Federal employees and contractor personnel associated with LM.
- g. LM Security Officer -- Designated LM representative who addresses custody, inquiries, and related activities in connection with instances of inadvertent disclosure of suspected Classified Information.
- h. Official Use Only (OUO) -- A designation identifying certain unclassified but sensitive information that may be exempt from public release under the Freedom of Information Act (FOIA); or a security classification marking used during the period July 18, 1949, through October 22, 1951.
- i. Program Records Official (PRO) -- Individual who ensures that all LM records management practices are properly executed.
- j. Proprietary Information -- Information that embodies trade secrets developed at private expense outside of a cooperative research and development agreement and commercial or financial information which is privileged or confidential under FOIA, 5 U.S.C. (B) (4).
- k. Protective Force -- Federal or contractor personnel assigned to protective duties involving DOE safeguards and security.
- l. Records Liaison Officer (RLO) -- Individual(s) designated by the PRO to oversee the LM records management program in cooperation with the DOE Records Officer.
- m. Sensitive Information -- Classified or Unclassified Controlled Information (see also Unclassified Controlled Information).
- n. Unauthorized Disclosure -- A communication or physical transfer of Classified Information or UCI to an unauthorized recipient.
- o. Unclassified Controlled Information (UCI) -- Unclassified information that may be exempt from public release under FOIA and for which disclosure, loss, misuse, alteration, or destruction may adversely affect national security, Governmental interests, or personal privacy.
- p. Unclassified Controlled Nuclear Information (UCNI) -- Certain unclassified Government information prohibited from unauthorized dissemination under section 148 of the Atomic Energy Act: (1) which concerns atomic energy defense programs; and (2) which pertains to the design of production facilities or utilization facilities; security measures (including security plans, procedures, and equipment) for the physical protection of production or utilization facilities; nuclear material contained in such facilities; or nuclear material in transit; the design, manufacture, or utilization of any nuclear weapon or component if the

design, manufacture, or utilization of such weapon or component was contained in any information declassified or removed from the Restricted Data category by the Assistant Secretary for Defense Programs (or the head of the DOE predecessor agency) pursuant to section 142 of the Atomic Energy Act; or whose unauthorized dissemination could reasonably be expected to significantly increase the likelihood of illegal production of nuclear weapons; or theft, diversion, or sabotage of nuclear materials, equipment, or facilities.

5. QUALITY CONTROL. The RLO shall review this procedure annually and as necessary to accommodate changing conditions within LM and to ensure compliance with applicable laws, regulations, and DOE requirements.
6. RESPONSIBILITIES.
 - a. The LM Security Officer is responsible for:
 - (1) Planning, organizing, training, directing, and controlling all aspects of the Classified and UCI protection and control program.
 - (2) Facilitating the destruction of LM Sensitive Information.
 - b. The RLO is responsible for:
 - (1) Communicating with the LM Security Officer concerning requests for UCI documents or questions concerning Classified or UCI documents.
 - (2) Recommending needed access and retrieval guidance to the PRO.
 - c. The Supervisor of an LM employee who discovers suspected Classified Information is responsible for:
 - (1) Assuming temporary control of the information and protecting it from further disclosure until the LM Security Officer is available to assume responsibility. If the LM Security Officer is not immediately available, the Supervisor works with cleared protective force personnel or a cleared DOE Federal or contractor employee (identified by a Q or L on their DOE badge) to take initial steps to protect information.
 - (2) Ensuring that related incident reports are properly completed.
 - d. LM personnel are responsible for understanding identification and protection requirements. When such exposure occurs, LM personnel work with their supervisor and the LM Security Officer to ensure safeguarding of the information.

7. TRAINING REQUIREMENTS.

- a. Personnel creating, using, or maintaining records shall be provided awareness training consisting of the annual security refresher briefing and the LM-specific OUO/UCNI training.
- b. Personnel who perform DOE-authorized work that involves contact with UCI and potential exposure to Classified Information shall be included in a security education program. All training must be developed in accordance with the requirements specified in DOE Order 470.4, Safeguards and Security Program and be tailored to the assigned duties and responsibilities of individuals receiving training.

8. DOCUMENT CONTROL.

- a. The Directives Manager shall maintain the official controlled version of this document in the LM ERKS.
- b. The Directives Manager shall place the most current version of this procedure on the LM Intranet for employee use.
- c. Printed hard copies of this document shall be considered information-only copies.
- d. The LM Security Officer shall use the current Government forms pertaining to this procedure.

9. PROCEDURE.

Attachment A. illustrates the process of identifying and protecting Sensitive Information.

a. **Classified Information**

In performance of its mission, LM does not assume custodianship of Classified Information. Transferred record collections may have Classified Information unintentionally commingled with unclassified material. If this occurs, LM personnel shall protect Classified Information from unauthorized disclosure following requirements in DOE Order 470.4, Safeguards and Security Program and DOE Manual 470.4-4, Information Security.

Identification

LM personnel identify OUO, UCI, UNCI, and Classified Information using computer-based training on the LM Intranet titled “OUO/UCNI Training,” the annual security refresher briefing, and material contained in Attachment B. – Classified Information Identification.

Protection (Inadvertent Disclosure Response)

Attachment C. illustrates the process of responding to incidents of inadvertent disclosure of Classified Information.

- (1) Upon discovery of information received by LM or contained in an LM records collection that appears to contain Classified Information, LM personnel immediately report the inadvertent disclosure to their Supervisor.
- (2) The Supervisor:
 - (a) Temporarily assumes responsibility for the situation. This includes securing the suspected Classified Information as a temporary protection measure.
 - (b) Arranges for immediate turnover and protection by transferring custody to one of the following LM representatives:
 - The LM Security Officer,
 - Cleared protective force personnel, or
 - A cleared DOE Federal or contractor employee (identified by a Q or L on their DOE badge).
 - (c) Ensures the LM Security Officer is notified of the situation.
- (3) The LM Security Officer:
 - (a) Takes custody of the suspected Classified Information and protects the information by locking it in an approved security container. If an approved security container is not available, the information must be placed in the most secure storage location possible.
 - (b) Conducts an inquiry according to DOE Manual 470.4-1, Safeguards and Security Program Planning and Management and determines if the incident warrants the issuance of a notice of security concern or security infraction.
 - (c) Forwards the information to the appropriate DOE organization for analysis.
 - (d) Ensures that information identified as Classified is transferred to an appropriate entity. [If it is determined that the information is not Classified, the LM Security Officer ensures that any needed

marking changes are made to the information so security concerns are not raised in the future, ensures that the information is returned to the proper record collection, and notifies the Supervisor as appropriate. No further action is needed.]

- (e) Informs the Supervisor by formal correspondence if findings of the inquiry constitute a security concern.
- (f) Completes any required reporting of the incident. This includes initiating DOE Form 5639.3, Report of Security Incident/Infraction. A copy of the incident report form is available on the DOE Directives Internet site.
- (g) Forwards the incident report form to the Supervisor.
- (4) The Supervisor completes Part 2 of the incident report form as instructed and returns the form to the LM Security Officer within 15 days of the inadvertent disclosure.
- (5) The LM Security Officer submits the completed incident report form to the appropriate DOE security office.
- (6) LM Personnel:
 - (a) Cooperate fully and provide accurate, truthful, and pertinent information when requested by the DOE Security Officer.
 - (b) Complete Standard Form SF-312, Classified Information Nondisclosure Agreement, as instructed.

b. Unclassified Controlled Information

LM record collections will contain the following types of information categorized as UCI:

- UCNI
- OUO information
- Proprietary Information

Identification

LM personnel identify UCI using computer-based training on the LM Intranet titled “OUO/UCNI Training” and material contained in Attachment D. – Unclassified Controlled Information Identification.

Protection

NOTE: Requests for UCNI documents must be in writing. Prior to external release of UCNI documents, the RLO submits the documents to the LM Security Officer, who shall have the originating program office review them to ensure the release will not compromise the goals and objectives of the program office. In cases where the originating office cannot be identified, the LM Security Officer shall send the documents to the appropriate DOE security office for review before release.

LM personnel shall take the following measures to protect UCI and prevent unauthorized access or disclosure:

- Store UCI in a building with Government or Government-contractor security. When such building security is not provided, locked rooms or locked file cabinets provide adequate protection.
- Restrict release of records/documents marked as containing UCI (including OUO, UCNI, and Proprietary) by persons who do not require the information to perform their official duties or other DOE-authorized activities. Reasonable precautions include not reading this information in public places.
- Take reasonable precautions with matter marked with the notice “MAY CONTAIN UCNI.” If there is a question as to whether a document actually contains UCNI, the RLO submits the document to the LM Security Officer, who arranges for a review to determine if UCNI is present.
- Confirm the citizenship of any person requesting access to UCNI. Persons accessing UCNI information must be U.S. citizens with a need to know the information for the completion of official duties or DOE-authorized activities. (Noncitizens may be able to access UCNI through creation of a specific security plan as coordinated by the LM Security Officer.)
- Contact the LM Security Officer for guidance if there is a question concerning an access request for UCI from an individual not normally authorized to access the information.
- Restrict the release of Proprietary Information. Proprietary Information cannot be released to individuals or organizations in competition with the information source without the permission of the source and the originator of the information.

Destruction of Unclassified Controlled Information

- (1) The LM Security Officer ensures destruction of specific UCI and ensures that destruction requirements are met. Detailed requirements concerning the destruction of UCI are included in DOE Manuals 471.3-1, Manual for Identifying and Protecting Official Use Only Information and 471.1-1, Identification and Protection of Unclassified Controlled Nuclear Information Manual.
- (2) LM Records Management personnel or authorized destruction vendors destroy UCI. Destruction may be accomplished by:
 - (a) Shredding using approved equipment (e.g., strip-cut shredders that result in particles or strips no more than ¼ -inch wide). Shredders used for UCI must be inspected and labeled by the LM Security Officer as being approved for Sensitive Information.
 - (b) Ensuring proper disposal of shredded particles. Properly shredded documents may be recycled. Unshredded documents may not be recycled.

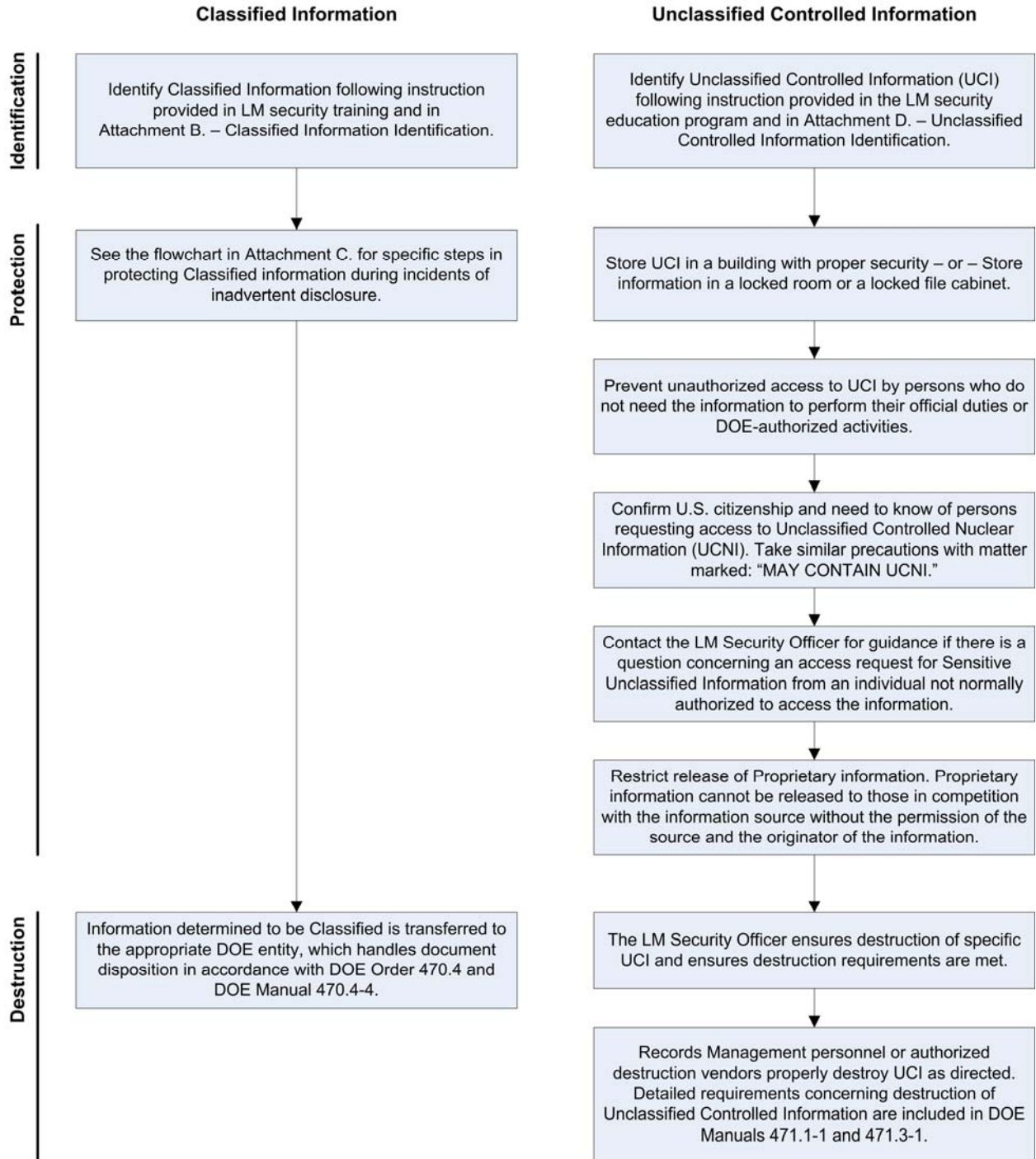
10. ATTACHMENTS.

- a. Attachment A. – Classified, Sensitive, and Proprietary Information Handling Flowchart
- b. Attachment B. – Classified Information Identification
- c. Attachment C. – Responding to Incidents of Inadvertent Disclosure of Classified Information
- d. Attachment D. – Unclassified Controlled Information Identification

Approved: Original signed by
Celinda H. Crawford
Director
Office of Business Operations

Distribution: As required

Attachment A. – Classified, Sensitive, and Proprietary Information Handling Flowchart



Attachment B. – Classified Information Identification

Legacy Management (LM) does not assume custodianship of any Classified Information. However, Classified Information may be inadvertently commingled with unclassified record collections transferred from closure sites.

To protect Classified Information from unauthorized disclosure, LM personnel who may be inadvertently exposed to Classified Information must be able to identify and recognize it. The following elements and examples are common to all Classified documents and should enable personnel to recognize that the information may be Classified:

a. Classification Level

The three classification levels are:

- **Top Secret (TS)** – Unauthorized disclosure could reasonably be expected to cause exceptionally grave damage to national security.
- **Secret (S)** – Unauthorized disclosure could reasonably be expected to cause serious damage to national security.
- **Confidential (C)** – Unauthorized disclosure could reasonably be expected to cause damage to national security.

The overall classification level of a document is marked on the top and bottom of the cover page (if any), on the title page (if any), on the first page, and on the outside of the back cover or last page. Each interior page of a Classified document is marked top and bottom with the highest classification level of that page or the overall classification of the document. These document markings are clearly distinguishable from the document text. Some unclassified information may contain “Unclassified” markings. These markings are sometimes used in areas where Classified and unclassified documents are stored together.

b. Classified Markings

The examples below show typical markings for a Classified document:

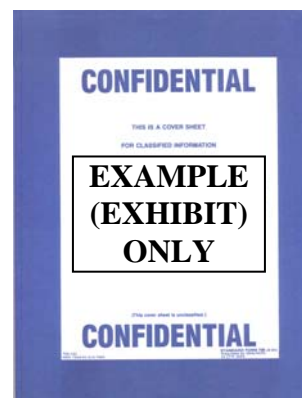
Cover Sheets:



SF-703
Orange/White



SF-704
Red/White



SF-705
Blue/White

Labels:



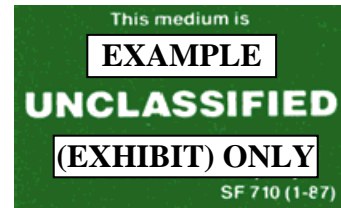
SF-706
Orange/White



SF-707
Red/White



SF-708
Blue/White



SF-710
Green/White
Label indicates the item is unclassified (used in mixed environments to identify unclassified media)

Document:

The highest classification level of information contained in an NSI document is placed at the top and bottom of the first page and on the back of the last page. [NOTE: The first page of a document is the first sheet of paper, either the cover page, title page, or first page of text, whichever comes first.] All other mandatory markings must also be displayed on the first page: caveats, classifier information, date, and originator identification, which includes the name and mailing address of the organization responsible for preparing the document. [NOTE: No category marking is used if the document contains only NSI.] For multi-page NSI documents, each interior page is marked at the top and bottom with the highest level of classified information contained in the document for example, Secret) or, if the document contains NSI and unclassified controlled information, each interior page may be marked according to the information contained on that page, either with the highest classification level of NSI, the appropriate unclassified controlled marking, or "Unclassified."

SECRET

LOREM IPSUM DOLOR SIT AMET, consectetur adipiscing elit. Nam sed risus. Sed quis volutpat venenatis, lacinia turpis vestibulum diam, vitae imperdiet sapien. neque et dui. Proin wisi.

SECRET

CLASSIFICATION OF THIS DOCUMENT IS FOR EXAMPLE PURPOSES ONLY

Classified By: Jill Freeze, Manager, Engineering Office
Derived From: CG-SS-4, September 12, 2000
Declassify On: X1, X4 and X5

INTERIOR PAGE

SECRET

ANEXUS UTILIQUE CLASSTORPER METUS. Cras vitae enim. Nulla interdum ultricies. enim. Riser lobortis. Praesent eu diam. Sed amet lorum volutpat velut. Praesent magna lorum, aliquet eu, conulacitiam sit, pretium sed, ante. Vivamus in dui.

SECRET

BACK OF LAST PAGE

SECRET

ALIQUEM ANEXUSUS IDEMUS. Conulacitiam massa. Sed eu odio in dui. Velut. Praesent. Praesent nulla lorum non lorum sceleris elementum.

SECRET

TOP SECRET

Department of Energy
Washington, D.C. 20588

July 1, 2002

MEMORANDUM FOR: GEORGE GREEN, DIRECTOR
OFFICE OF ADMINISTRATIVE SERVICES

FROM: JOE COOL, DIRECTOR
ENGINEERING DIVISION

SUBJECT: Accountable Derivatively Classified Top Secret NSI Document (U)

(U) This example identifies the preferred marking of a derivatively classified Top Secret NSI document.

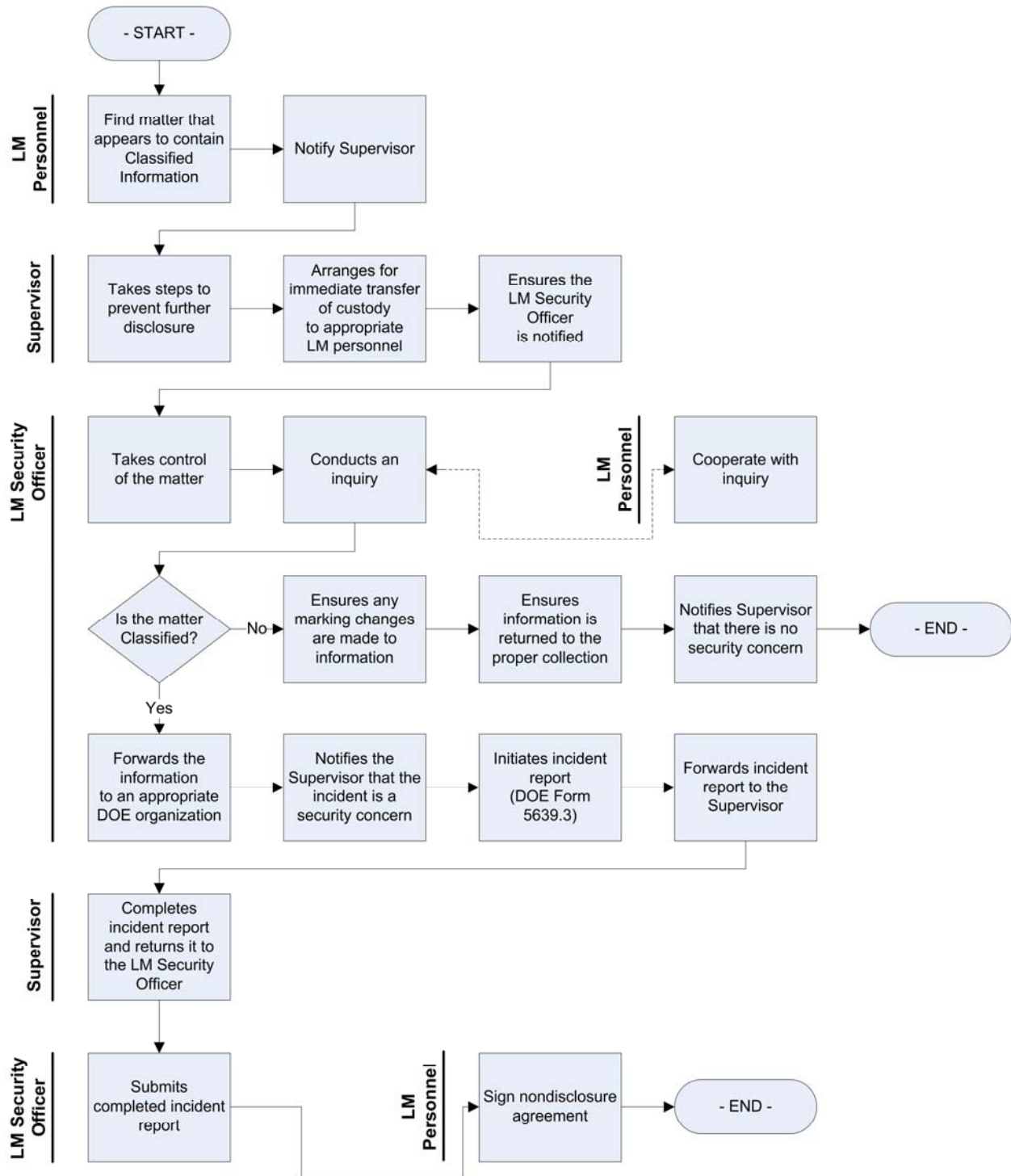
- (U) **Level and Category Markings.** The highest classification level of information contained in the document is placed at the top and bottom of the first page and on the back of the last page. [NOTE: No category marking is used if the document contains only NSI.] For multi-page documents, each interior page is marked at the top and bottom with the highest level of information contained in the document for example, Top Secret) or, if the document contains NSI and unclassified controlled information, each interior page may be marked according to the information contained on that page, either with the highest classification level of NSI, the appropriate unclassified controlled marking, or "Unclassified."
- (U) **Classifier Markings.** Classifier information is placed at the lower left corner of the first page of the document. This includes the following:
Classified By: Name or personal identifier and position title. If the signer of the document is also the classifier, the word "signer" may be used on the "Classified By" line.
Derived From: Designation of the guide or source documents and date of such documents.
Declassify On: Date or event 10 years or less from the date of the document or the letter "X" and the exemption category number. This information is obtained from the classification guide or source document.
- (U) **Accountability Markings.** Top Secret documents are considered accountable documents and are assigned a unique identification number. This unique identification number must be placed on the first page of the document, preferably in the upper right corner.
- (TS) **Portion Markings.** Portion markings are required for each document containing only NSI. The markings must be placed immediately preceding the portions to which they pertain. If the portion has a number, letter, or bullet, then the markings must follow the number, letter, or bullet of the portion. Portions should be marked to indicate the level of classification (TS, S, or C), any caveats, or whether they contain unclassified controlled information or are unclassified (U).
- (C) **Subject/Title Marking.** The subject or title of each NSI document must be marked to identify the classification level, any caveats, or whether it contains unclassified controlled information or is unclassified. This marking is placed after the subject or title.
- (U) **Automatic Declassification Exemption.** If a document is marked as exempt from automatic declassification on the "Declassify On" line, each classified portion of that document is presumed to also be exempt.

Classified By: Signer
Derived From: CG-SS-4, Sept. 12, 2000
Declassify On: X1 and X5

TOP SECRET

The most recent and official controlled hard copy version of this document resides with LM's Directives Coordinator. An electronic version of the controlled document has been placed on the LM Intranet for employee use. Printed hard copies of this electronic version are considered uncontrolled documents.

Attachment C. – Responding to Incidents of Inadvertent Disclosure of Classified Information



Attachment D. – Unclassified Controlled Information Identification

a. Categories and Formats

Legacy Management (LM) record collections will contain the following types of information categorized as Unclassified Controlled Information (UCI). UCI can be in the following formats:

- Handwritten, printed, or typed matter;
- Photographic prints, exposed or developed film, or motion pictures;
- Automated information system input and equipment content including memory, visual displays, computer printouts, disks or diskettes, or hard disk drives; and
- Audio and video recordings.

b. Unclassified Controlled Nuclear Information (UCNI) Markings

The following examples show typical markings for UCNI:

For information that formerly was UNCI:

**DOES NOT CONTAIN UNCLASSIFIED CONTROLLED
NUCLEAR INFORMATION**

Reviewing Official: _____
(Name/Organization)

Date: _____

For information that may contain UCNI:

Not for Public Dissemination

May contain Unclassified Controlled Nuclear Information
subject to section 148 of the Atomic energy Act of 1954, as
amended (42 U.S.C. 2168). Approval by the Department of
Energy prior to release is required.


For information containing UCNI:

Unclassified Controlled Nuclear Information
Not for Public Dissemination
Unauthorized dissemination subject to civil and criminal
sanctions under section 148 of the Atomic Energy Act of
1954, as amended (42 U.S.C. 2168)

or

Not for Public Dissemination
Unauthorized dissemination subject to civil and criminal
sanctions under 42 U.S.C. 2168.

Example of document containing UCNI:

	UNCLASSIFIED CONTROLLED NUCLEAR INFORMATION Department of Energy Washington, D.C. 20585	<div style="border: 1px solid black; padding: 2px; font-size: 0.8em;"> MARKINGS ON THIS DOCUMENT ARE FOR EXAMPLE PURPOSES ONLY </div>
July 1, 2002		
MEMORANDUM FOR FROM: SUBJECT:	GEORGE GREEN, DIRECTOR OFFICE OF ADMINISTRATIVE SERVICES JOE COOL, DIRECTOR ENGINEERING DIVISION Unclassified Controlled Nuclear Information Markings	
<p>This memorandum illustrates the proper marking of a document that has received a review by an UCNI Reviewing Official and has been determined to contain UCNI.</p> <p>A Reviewing Official determines that an unclassified document contains UCNI based on applicable topical or internal guidelines and ensures that the front of the document is marked as indicated below.</p> <p>The marking "UNCLASSIFIED CONTROLLED NUCLEAR INFORMATION" or "UCNI" must be placed on the top and bottom of the front of the document and on the top and bottom of each interior page of the document or, if more convenient, on the top and bottom of only those interior pages that contain UCNI. The UCNI front marking, showing the name and organization of the Reviewing Official, the date of review, and the guidance used, is placed on the first page of the document preferably in the lower lefthand corner.</p>		
UNCLASSIFIED CONTROLLED NUCLEAR INFORMATION NOT FOR PUBLIC DISSEMINATION Unauthorized dissemination subject to civil and criminal sanctions under Section 148 of the Atomic Energy Act of 1954, as amended (42 U.S.C. 2168). Reviewing Official: <u>Ray Holmer, SO-113</u> Date: <u>1 July 2002</u> Guidance Used: <u>CG-88-4, Sept. 12, 2000</u>		
UNCLASSIFIED CONTROLLED NUCLEAR INFORMATION		

c. Official Use Only (OUO) Markings

The following example shows typical markings for OUO information:


OFFICIAL USE ONLY

May be exempt from public release under the Freedom of Information Act
(5 U.S.C. 552), exemption number and category: _____

Department of Energy review required before public release

Name/Org: _____ Date: _____

Guidance (if applicable) _____

	Department of Energy Washington, D.C. 20585 July 1, 2002	MARKINGS ON THIS DOCUMENT ARE FOR EXAMPLE PURPOSES ONLY
<p>MEMORANDUM FOR SAFEGUARDS AND SECURITY DIRECTORS</p> <p>FROM: JOSEPH S. MAHALEY, DIRECTOR OFFICE OF SECURITY</p> <p>SUBJECT: Applying Official Use Only (OUO) Marking</p> <p>The concept of identifying certain sensitive Government information as being OUO has a long and varied history. Until July 18, 1949, OUO was widely applied to all kinds of unclassified but sensitive Government information not intended for public release. From then until October 23, 1951, it was a fourth classification level below Confidential and was similar to the Restricted level still used by many other countries. As a result, any document marked "OUO" from July 18, 1949, through October 22, 1951, must be reviewed by a classifier prior to release to ensure it is not actually classified.</p> <p>For information to be identified as OUO, it must be unclassified; fall under at least one of eight Freedom of Information Act (FOIA) exemptions (i.e., exemptions 2 through 9; information falling under exemption 1 can never be OUO because it covers information classified by Executive order); and have the potential to damage governmental, commercial, or private interests if disseminated to persons who do not need to know the information to perform their jobs or other DOE-authorized activities. The employee determining that a document contains OUO information must ensure that the document is marked as illustrated on this example.</p> <p>The front marking (containing the applicable FOIA exemption number, the related category name, the name and organization of the employee making the determination, and the date of the determination) is applied to the front of the document (preferably in the lower lefthand corner). Additionally, the words "Official Use Only" (or "OUO" if space is limited) are placed on the bottom of the front page as well as on each interior page or, if more convenient, on just those interior pages containing the OUO information.</p>		
OFFICIAL USE ONLY May be exempt from public release under the Freedom of Information Act (5 U.S.C. 552), exemption number and category: 2, Circumvention of Statute		
Department of Energy review required before public release Name/Org: Ray Holmer, SO-113 Date: 12/6/02 Guidance (if applicable) ---		

d. **Proprietary Markings**

Information may be marked with the word “Proprietary” or it may be unmarked.

The most recent and official controlled hard copy version of this document resides with LM's Directives Coordinator. An electronic version of the controlled document has been placed on the LM Intranet for employee use. Printed hard copies of this electronic version are considered uncontrolled documents.